Quantum Supremacy and Post-Quantum Cryptography Equity: Toward a Fair Digital Future

Quantum computing is knocking on the door of the future. Google's Sycamore and China's Jiuzhang completed tasks in 200 seconds that would take classical computers thousands or even 600 million years, marking the era of "Quantum Supremacy." But as quantum computers threaten the security of traditional cryptographic systems, who will hold the keys to data security? A handful of tech giants, or everyone? This article introduces, for the first time globally, the concept of "Post-Quantum Cryptography Equity" (PQC Equity), envisioning a world where post-quantum cryptography becomes as ubiquitous as Wi-Fi, accessible to everyone.

1. Quantum Supremacy: Breakthroughs and Concerns

Quantum supremacy represents a leap in quantum computing. Leveraging quantum superposition and entanglement, quantum computers can achieve exponential speedups for specific tasks. The successes of Google's Sycamore and China's Jiuzhang demonstrate quantum computing's potential, attracting global investment and heralding revolutions in supply chains, finance, and data security.

However, quantum supremacy comes with concerns. While current achievements are largely theoretical, their practical utility remains limited. More critically, quantum technology is concentrated in the hands of a few nations and corporations, potentially widening the technological divide. If only giants can harness quantum power, small and medium-sized enterprises (SMEs) and individuals face heightened risks, as traditional cryptographic systems can no longer secure commercial or personal data.

2. Post-Quantum Cryptography: The Foundation of Quantum Security

The rise of quantum computing threatens traditional cryptographic systems. Shor's algorithm can easily break RSA, ECC, and SM2 algorithms, which underpin global internet security. Post-Quantum Cryptography (PQC), based on new mathematical challenges like lattice-based cryptography and hash-based signatures, has emerged to counter quantum attacks. In August 2024, the U.S. National Institute of Standards and Technology (NIST) released its first three PQC standards for key encapsulation and digital signatures, accelerating their adoption in products and services.

Yet, deploying PQC presents challenges. Systems require upgrades, and PQC algorithms may increase computational demands by 50%, a burden SMEs and IoT devices may struggle to bear. High migration costs and lengthy timelines could leave developing nations and smaller organizations with data effectively unprotected in the quantum era. How can we ensure quantum computing doesn't become the privilege of a few? The answer lies in "Post-Quantum Cryptography Equity."

3. Post-Quantum Cryptography Equity: A Fair Digital Future

The concept of "Post-Quantum Cryptography Equity," proposed here, envisions universal access to quantum-resistant cryptography, ensuring that every organization - regardless of size or resources -and every individual can secure their data in the quantum era. This prevents the "harvest now, decrypt later" threat, safeguarding commercial and personal data. Global cybersecurity leader Cloudflare has taken a bold step, stating in its official blog on March 17, 2025: "We believe privacy is a fundamental human right, and advanced cryptography should be accessible to everyone without compromise. No one should be required to pay extra for post-quantum security." Cloudflare not only realizes the SSL certificate automation management, but also has upgraded its CDN services to support post-quantum cryptography HTTPS encryption for all users at no cost. I applaud Cloudflare, alongside Google Chrome, for pioneering PQC Equity globally.

Achieving this vision requires collective effort:

(1) Open-Source Algorithms: Projects like Open Quantum Safe, OpenSSL project, TongsuoSSL project, openHiTLS project provide free PQC libraries, lowering technical barriers.

(2) Global Standardization: NIST and ETSI's efforts need global enterprise participation to ensure standards are compatible across systems and services.

(3) Automatic Implementation: Free, seamless upgrade solutions for PQC support with zero system modifications.

(4) Education and Awareness: Training and outreach to inform businesses and the public about

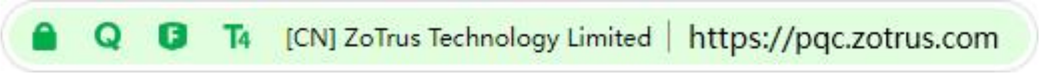
the importance and urgency of adopting PQC.

PQC Equity is not just a technical goal but a corporate social responsibility. Technological progress should not come at the cost of fairness. Enterprises must ensure security benefits everyone, protecting personal and commercial data in the quantum era, rather than becoming the privilege of a few wielding quantum supremacy.

4. ZoTrus Technology: A Champion of PQC Equity

ZoTrus Technology has prioritized PQC research, becoming a member of the PKI Consortium in February 2023 and one of the earliest participants in its PQC working group. On August 8, 2025, it announced a timeline for its post-quantum cryptography HTTPS application ecosystem, marking a significant step toward PQC Equity.

A flagship product in this ecosystem is ZT Browser, a free, ad-free browser supporting SM2 algorithm. Its upcoming version 137 will support post-quantum cryptography algorithm for HTTPS encryption, prioritizing PQC algorithms and introducing a global first: a post-quantum cryptography icon (**Q**) next to the padlock icon in the address bar, see below figure. This allows ZT Browser users to instantly recognize whether a website uses post-quantum cryptography HTTPS encryption, ensuring their data remains secure in the quantum era.



[CN] ZoTrus Technology Limited | https://pqc.zotrus.com

All ZT Browser users will receive free automatic upgrades to PQC support, as ZoTrus Technology, like Cloudflare, believes users shouldn't pay extra for quantum security. This innovative UI also serves as PQC education, bringing advanced cryptography into the public eye and encouraging websites to adopt PQC, ensuring data security now and in the quantum future.

Another key product is ZoTrus HTTPS Automation Gateway, a client-to-cloud integration solution enabling zero-modification Web server support for dual-algorithm (ECC and SM2) SSL certificate automation management. This lays the technical foundation for seamless migration to PQC HTTPS encryption. All users of the Gateway will transition to PQC HTTPS encryption effortlessly and at no cost, reinforcing ZoTrus Technology's commitment to PQC Equity.

5. Action Shapes the Future

Quantum supremacy ignites a technological revolution, but PQC Equity determines its inclusivity. Quantum supremacy is like the breakthrough of high-speed rail; PQC Equity ensures everyone can ride it. Cloudflare’s free post-quantum cryptography HTTPS encryption via CDN and ZoTrus Technology’s innovations in Browser and Gateway fill critical gaps in the equity ecosystem, focusing on automation and user-friendly experience. Their efforts to prove a fair digital future are within reach. The author calls on more enterprises to join this mission: invest in post-quantum cryptography technologies, support open-source initiatives and standardization, embrace SSL certificate automation management, and actively prepare for PQC migration.

As a leader in SSL certificate automation management, ZoTrus Technology’s responsibility extends beyond technological advancement to ensure its benefits reach everyone. Let’s work together to make post-quantum cryptography HTTPS encryption universally accessible, building a secure and equitable quantum future where the keys to quantum security are in everyone’s hands.

Richard Wang

August 18, 2025
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 99 articles in English (more than 134K words)
and 224 articles in Chinese (more than 669K characters in total).